computer code that when executed on a computer causes the computer to decrypt the data packet using the encryption method.

69. The system as recited in claim 16, wherein the mechanism indirectly references said predetermined encryption/decryption mechanism.

70. The system as recited in claim 20, wherein the mechanism indirectly identifies the encryption method.

71. The method as recited in claim 26, wherein the mechanism indirectly identifies the encryption method.

72. The computer program product as recited in claim 36, wherein the mechanism indirectly identifies the encryption method.

73. The computer system as recited in claim 38, wherein the mechanism indirectly identifies the encryption method.

REMARKS

In the Office Action, the Examiner objected to claims 6, 14, and 22-25, and rejected claims 1-53 under 35 USC § 251, 35 USC § 101, 35 USC §112 and under 35 USC §102. These objections and rejections are fully traversed below.

The claims have been amended to correct minor informalities and to further clarify the subject matter regarded as the invention. Claims 1-73 are now pending.

Reconsideration of the application is respectfully requested based on the following remarks.

SUPPLEMENTAL DECLARATION

A supplemental declaration is being prepared by Applicant. Applicant will submit the new declaration after it is properly executed.

OBJECTION TO CLAIMS 6, 14, AND 22-25

In the Office Action, the Examiner objected to claims 6, 14, and 22-25 due to various informalities. The claims are amended in accordance with the Examiner's recommendations. However, with respect to claim 14, Applicant believes that "said at least one predetermined criterion" most accurately claims the subject matter which Applicant regards as the invention. Hence, Applicant respectfully requests that the Examiner withdraw the objection to claims 6, 14, and 22-25.

REJECTION OF CLAIMS 26-53 UNDER 35 USC §251

In the Office Action, the Examiner rejected claims 26-53 under 35 USC §251 as being an improper recapture of claimed subject matter cancelled in the application for the patent upon which the present reissue is based. Applicant has amended claims 26-39 to recite the generation of a new header during the encryption of a data packet. However, since claims 40-53 are directed to decryption of a data packet, the generation of a new address header need not be recited. Therefore, there is no recapture of claimed subject matter cancelled in the application for the patent on which the present reissue is based. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejection to claims 26-53 under 35 USC §251.

REJECTION OF CLAIMS 36-37 AND 50-51 UNDER 35 USC §101

In the Office Action, the Examiner rejected claims 36-37 and 50-51 under 35 USC §101 because they are non-statutory. The claims have been amended such that they recite patentable subject matter. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejection to claims 36-37 and 50-51 under 35 USC §101.

REJECTION OF CLAIMS 1-15, 17-21, 30-33, 36-39, 44-46, AND 50-53 UNDER 35 USC §112

In the Office Action, the Examiner rejected claims 1-15, 17-21, 30-33, 36-39, 44-46, and 50-53 under 35 USC §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. The claims are amended in accordance with the Examiner's recommendations. However, with respect to claim 18, Applicant was unable to discern an inconsistent use of the terms "data packet" in lines 11 and 14. Hence, Applicant respectfully requests that the Examiner withdraw the rejection of claims 1-15, 17-21, 30-33, 36-39, 44-46, and 50-53 under 35 USC §112, second paragraph.

REJECTION OF CLAIMS 1-53 UNDER 35 USC §102

In the Office Action, the Examiner rejected claims 26, 27, and 29 under 35 USC §102(b) as being anticipated by Carter et al., U.S. Patent No. 5,161,192, ('Carter' hereinafter). In addition, the Examiner rejected claims 1, 6, 11, 13-18, 26-29, 34-39, 40-43, and 48-53 under 35 USC §102(e) as being anticipated by Adams Jr. et al., U.S. Patent No. 5,442,708, ('Adams' hereinafter). In addition, the Examiner rejected claims 1-53 under 35 USC §102(e) as being anticipated by Adams Jr. et al., U.S. Patent No. 5,444,782, ('Adams Jr.' hereinafter). These rejections are fully traversed below.

Carter discloses a repeater that reads a portion of each frame, which may be all or part of the destination address segment and/or of the source address segment. See Carter, Abstract. It compares the data that it reads with stored access rules to determine whether the frame is permitted or not. See Carter, Abstract. If not, the repeater modifies the frame, for example by overwriting it with meaningless digits or by encrypting it. See Carter Abstract.

Adams discloses a computer network encryption/decryption device (CNEDD) that operates by selectively encrypting or decrypting only the data portion of a data packet, leaving the routing information contained in the header portion of the data packet unchanged. See Adams, Abstract. The CNEDD examines the header of a packet and consults a table which includes handling instructions for the packet based on source, destination or other information provided in the header. See Adams, col. 4, lines 57-64; col. 6, lines 32-36. More particularly, the table includes matching criteria that contains source and destination

addresses, and other information. See Adams, col. 6, lines 37-41. In addition, the table may contain a plurality of keys used for encryption and decryption. See Adams, col. 6, lines 42-43. The table is described as further including handling instructions. See Adams, col. 6, lines 43-46.

Adams Jr. discloses a computer network encryption/decryption device (CNEDD) that operates in one of two modes by selectively encrypting or decrypting packets based on information contained in a packet's header. See Adams Jr., Abstract. When the CNEDD operates in the standard mode, only the data portion of a packet is encrypted, and a new packet is transmitted which includes an unencrypted header (with the original routing information) and the encrypted data. See Adams Jr., col. 6, lines 63-68. In the tunneling mode, both the data characters and the header characters of a packet are encrypted. See Adams Jr., col. 6, line 68 – col. 7, line 2. In addition, encryption and decryption is performed based on information contained in a table, as described in Adams. See Adams Jr., col. 7, lines 17-41. Rather than including the routing information from the original data packet in the header of the encrypted packet, the header indicates that the source of the packet is a CNEDD and the destination of the packet is a CNEDD in the network which contains the intended target node. See Adams Jr., col. 9, line 57-col. 10, line 2.

Header of encrypted data packet identifying encryption method used to encrypt the data packet

Claims 1, 6, 11, 16, and 17, as amended, are drawn to a method or system adapted for encrypting a data packet according to a predetermined encryption/decryption mechanism, generating a new header including a mechanism for identifying the predetermined encryption/decryption mechanism and appending the new header to the encrypted data packet.

Similarly, claims 20 and 24 are drawn to a method or system for decrypting a data packet including a header that includes a mechanism for identifying an encryption method used to encrypt the data packet.

Claims 26, 36, and 38, as amended, are drawn to a method, computer program product, or computer system adapted for encrypting data packets. When a data packet is encrypted, a new header is generated and appended to the encrypted data packet. The new

header includes a mechanism for identifying an encryption method used to generate the encrypted data packet. As a result, the presently claimed invention permits the encryption method to be tailored for each packet transmitted rather than requiring that the encryption method be specified statically (e.g., according to the source and/or destination of the packet).

None of the cited references, separately or in combination, discloses or suggests identifying an encryption method in a header of the encrypted data packet. Similarly, none of the cited references discloses or suggests decrypting a data packet that has a header including a mechanism for identifying the encryption method used to encrypt the data packet. Accordingly, claims 1, 6, 11, 16, 17, 20, 24, 26, 36, and 38 are patentable over Adams and Adams Jr.

Header of encrypted data packet identifying broadcast addresses of the networks associated with the source and destination of the data packet

Claims 7 and 14, as amended, are drawn to a system adapted for encrypting a data packet transmitted from a first host computer on a first computer network to a second host computer on a second computer network, and for generating and appending a new header to the encrypted data packet. Moreover, the new header identifies broadcast addresses of the networks associated with the host computers.

Claims 32 and 33 are similarly drawn to a method of encrypting data packets in which an identifier of the network associated with either the source host computer or the destination host computer, respectively, is included in the new header.

Similarly, claims 18, 22, 40, 50, and 52, as amended, are drawn to a method, system, computer program product, or computer system adapted for decrypting a data packet sent from a source to a destination. The data packet has a header identifying broadcast addresses of the source and the destination.

In contrast, Adams discloses that the routing information contained in the header portion of the data packet remains unchanged. Thus, Adams neither discloses nor suggests appending a new header including the internetwork broadcast addresses of either the source or the destination host computers to the encrypted data packet. Similarly, Adams neither

discloses nor suggests decrypting a data packet having a header identifying broadcast addresses of either the source or the destination. Accordingly, claims 7, 14, 18, 22, 32, 33, 40, 50, and 52 are patentable over Adams.

Although Adams Jr. suggests that the routing information included in the original data packet may be modified, Adams Jr. states that it is preferred that the new header indicates that the source of the packet is a CNEDD and the destination of the packet is a CNEDD in the network which contains the intended target node. See Adams Jr., col. 9, line 66 – col. 10, line 2. Adams Jr. neither discloses nor suggests that the new header include broadcast addresses of the source and the destination rather than the addresses of the devices that are responsible for encryption and decryption of the data packet. The presently claimed invention therefore provides greater protection against tapping into the network to decipher the nature of the information transmitted. Accordingly, claims 7, 14, 18, 22, 32, 33, 40, 50, and 52 are patentable over Adams Jr.

SUPPORT FOR NEW CLAIMS AND AMENDMENTS

Col. 6, lines 12-16 and lines 26-28 provide support for claims in which the broadcast addresses of the networks associated with the source and destination of the data packet may be identified in a header of the data packet. In addition, key management information such as information indicating which encryption scheme was used may be provided in a header to the data packet. See col. 6, lines 12-20. Col. 6, lines 21-25 state that the key management information 440 as well as the original data packet 400 are encrypted in mode 2. Support for specification of correlation data and encryption rules is disclosed in col. 4, lines 30-67.

SUMMARY

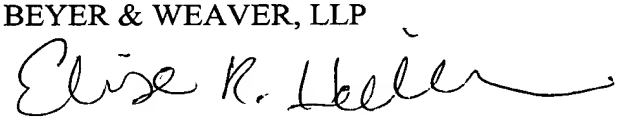
Dependent claims 2-5, 8-10, 12-13, 15, 19, 21, 23, 25, 27-31, 34-35, 37, 39, 41-49, 51, and 53 depend from one of independent claims 1, 6, 7, 11, 14, 16, 17, 18, 20, 22, 24, 26, 32, 33, 36, 38, 40, 50, and 52 and are therefore patentable over Adams and Adams Jr. for at least the same reasons. However, the dependent claims recite additional limitations that further distinguish them from the cited references. Hence, it is submitted that dependent claims 2-5, 8-10, 12-13, 15, 19, 21, 23, 25, 27-31, 34-35, 37, 39, 41-49, 51, and 53 are patentably distinct from Adams and Adams Jr.

Based on the foregoing, it is submitted that claims 1, 6, 7, 11, 14, 16, 17, 18, 20, 22, 24, 26, 32, 33, 36, 38, 40, 50, and 52 are patentably distinct from Adams and Adams Jr. In addition, it is submitted that dependent claims 2-5, 8-10, 12-13, 15, 19, 21, 23, 25, 27-31, 34-35, 37, 39, 41-49, 51, and 53 are also patentably distinct for at least the same reasons. The additional limitations recited in the independent claims or the dependent claims are not further discussed as the above discussed limitations are clearly sufficient to distinguish the claimed invention from Adams and Adams Jr. Thus, it is respectfully requested that the Examiner withdraw the rejection of claims 1-53 under 35 USC §102(e). Reconsideration of the application and an early Notice of Allowance are earnestly solicited.

If there are any issues remaining which the Examiner believes could be resolved through either a Supplemental Response or an Examiner's Amendment, the Examiner is respectfully requested to contact the undersigned attorney at the telephone number listed below.

Applicants hereby petition for an extension of time which may be required to maintain the pendency of this case, and any required fee for such extension or any further fee required in connection with the filing of this Amendment is to be charged to Deposit Account No. 50-0388 (Order No. SUN1P342R).

Respectfully submitted,
BEYER & WEAVER, LLP



Elise R. Heilbrunn
Reg. No. 42,649

BEYER & WEAVER, LLP
P.O. Box 61059
Palo Alto, California 94306
Tel. (510) 843-6200